713-TP-001-001

DAAC Addressing Study for the ECS Project

Technical Paper

March 2001

Prepared Under Contract NAS5-60000

RESPONSIBLE AUTHOR

Randy Haynes /s/ 3/30/01

Randy Haynes, Systems Engineering Date
EOSDIS Core System Project

RESPONSIBLE OFFICE

James Mather /s/ 3/30/01

James Mather, Hardware Engineering Date
EOSDIS Core System Project

Raytheon Company
Upper Marlboro, Maryland

This page intentionally left blank.

Abstract

The ESDIS project is considering re-addressing the DAAC Production networks to allow NASA greater network provider flexibility.

This paper evaluates the design trade-offs in how to implement this strategy once the firewalls are installed. A recommended implementation is presented.

Keywords: DAAC network, Production network, EMSnet, readdressing

This page intentionally left blank.

Contents

Abstract

Contents

1. Introduction

2. Design Trade-offs

3. EDC DAAC

4. NSIDC DAAC

List of Figures

Abbreviations and Acronyms

1. Introduction

1.1 Purpose

This study will examine different strategies to support re-addressing of the Production network and its connectivity to EMSnet (ESDIS Mission Support network). EMSnet is also known as EBnet.

While this study can apply to any DAAC, it is limited to only the EDC and NSIDC DAACs. These DAACs are not located at NASA facilities and will require the use of non-NASA communication circuits when network bandwidth requirements increase. However, the analysis presented in this paper also applies to the other DAACs, VATC, and PVC. The tasks would be the same but the duration of each task could vary.

1.2 Organization

This paper provides the following:

- A definition of the External and Internal DAAC Networks.
- Two readdressing strategies.
- A strategy recommendation.
- Identification of site-specific tasks.

It includes the following Sections:

1. Introduction
2. Design Trade-offs
3. EDC DAAC (implementation tasks)
4. NSIDC DAAC (implementation tasks)

Questions regarding technical information contained within this Paper should be addressed to the following ECS contact:

- ECS Contacts
  - Randy Haynes, Systems Engineering, 301-925-0932, rhaynes@eos.hitc.com

Questions concerning distribution or control of this document should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Systems Company
1616 McCormick Drive
Upper Marlboro, MD 20774-5301

2. Design Trade-offs

2.1 Introduction

There are two potential strategies for readdressing the EDC and NSIDC DAACs. One strategy is to modify the external and internal DAAC network addresses and the other is to only modify the external DAAC network addresses.

Before these strategies can be discussed, the external and internal DAAC networks needs to be defined.

2.2 DAAC Network Definitions

2.2.1 External

The external DAAC network is defined as the Production network address space which is outside of the DAAC firewall and ECS router. This is where the DAAC peers with EMSnet. See Figure 2-1, DAAC Network with Firewall diagram, for details.

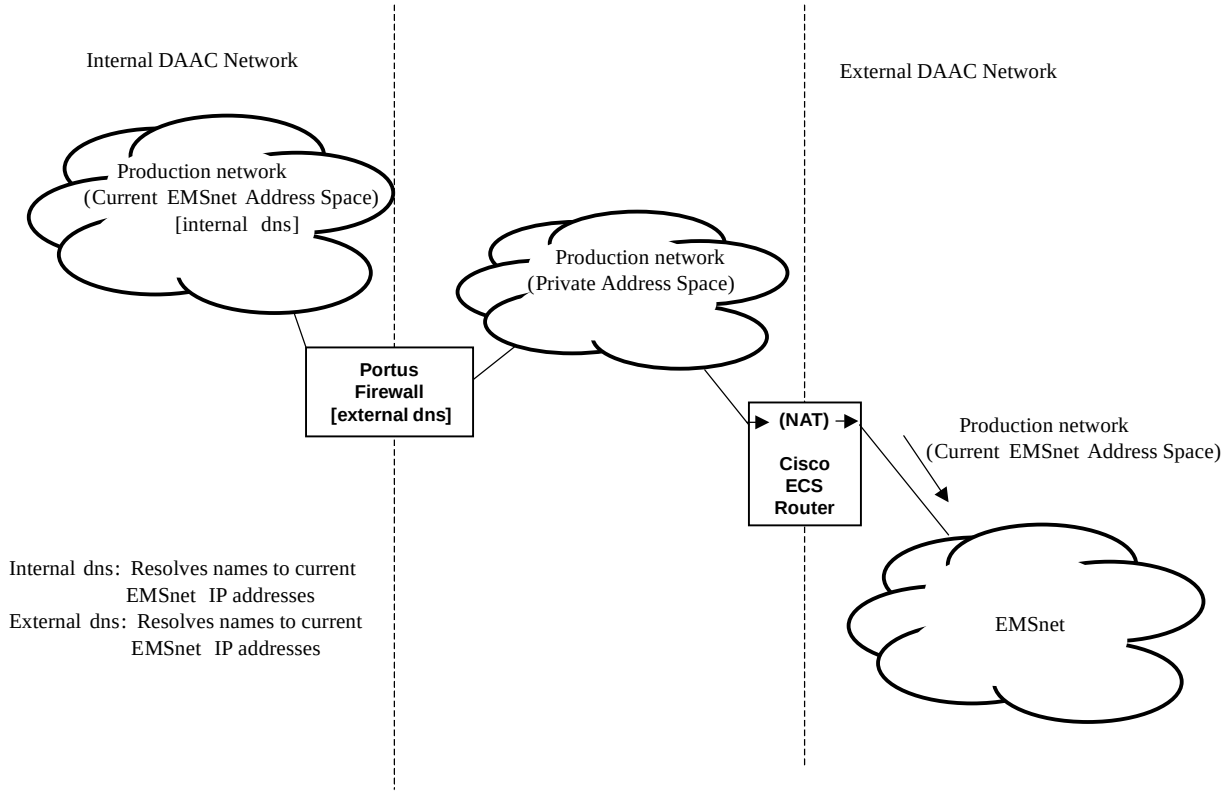

Figure 2-1. DAAC Network with Firewall

2.2.2 Internal

The internal DAAC network is defined as the Production network address space which is inside of the DAAC firewall. It does not directly peer with EMSnet. Its only external communication is to the inside of the firewall. See Figure 2-1, DAAC Network with Firewall diagram, for details.

2.3 Readdress Internal and External DAAC Networks Strategy

2.3.1 Description

This strategy is to modify both the internal and external DAAC network address space. The internal DAAC address space would be converted to private address space as defined in RFC 1878. The external DAAC network address space would be converted to the new network provider's address space.

Because the DCE database can easily become corrupted when changing IP addresses, the DAACs will not allow IP addresses to be changed until DCE has been removed.

The DAAC would be down from 24-to-48 hours to implement this strategy. All work required by Landover personnel would be performed via remote logins.

2.3.2 Dependencies

This implementation is dependent on the following:

a. Network peering with EMSnet is no longer via NASA provided circuits.

b. Firewall deployed.

c. DCE removed from ECS.

2.3.3 Cost

The tasks required to implement this strategy are defined for EDC in sections 3.1 and 3.2, and for NSIDC in sections 4.1 and 4.2.

The cost for each DAAC is identified in a separate ROM associated with this technical paper.

2.4 Readdress Only External DAAC Network Strategy

2.4.1 Description

This strategy is to only modify the external DAAC network address space. The external DAAC network address space would be converted to the new network provider's address space.

The internal DAAC address space would continue using its current address space. While using private address space as defined in RFC 1878 is the right choice for new network installations, it is not necessary when converting a network. This is only true if the network does not directly communicate with the outside world (i.e. remains an internal network behind a firewall).

Because the internal DAAC network becomes a private network, it does not matter what IP addresses it has. Keeping the current NISN IP addresses within the internal DAAC network has no impact on what the external DAAC IP addresses are. The firewall translates between the internal and external addresses.

The DAAC would be down for less than 24 hours to implement this strategy

There would be no travel required. The work required by Landover personnel would be performed via remote logins.

2.4.2 Cost

The tasks required to implement this strategy are defined for EDC in section 3.1, and for NSIDC in section 4.1.

The cost for each DAAC is identified in a separate ROM associated with this technical paper.

2.4.3 Dependencies

This implementation is dependent on the following:

a. Network peering with EMSnet is no longer via NASA provided circuits.

b. Firewall deployed.

2.5 Recommendation

ECS recommends that the strategy to only modify the external DAAC network addresses as defined in section 2.4 be implemented. This is due to the amount of work required (as defined in sections 3.2 and 4.2) to re-address the internal DAAC's Production networks, the length of time the DAAC will be unavailable, and dependence on removal of DCE.

This page intentionally left blank.

3. EDC DAAC

3.1 Readdress External DAAC Network Tasks

The tasks defined in this section assume that the firewall has already been implemented. The knowledge gained about all external interfaces discovered during the firewall design and implementation are used for this task. See Figure 3-1, EDC DAAC Network with Firewall diagram, for details.

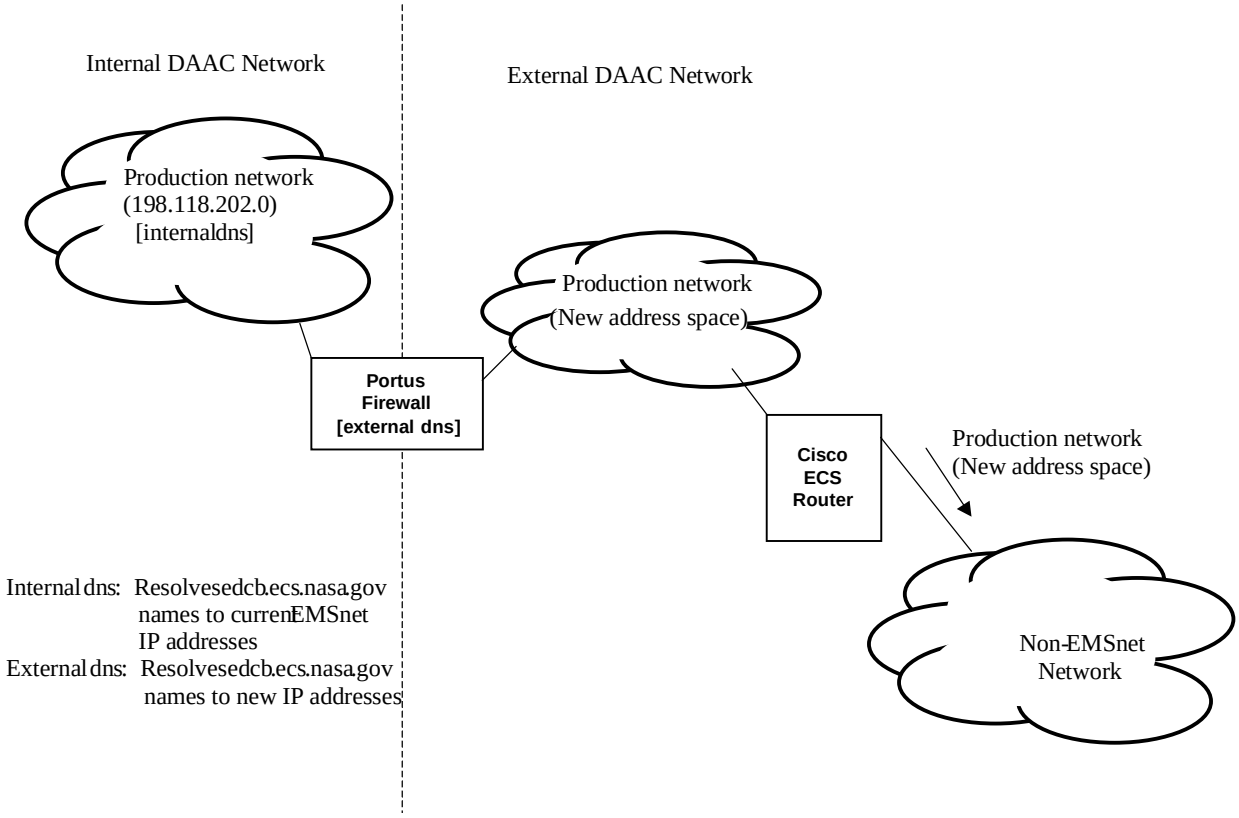

Figure 3-1. EDC Network with Firewall

The following tasks will be performed to readdress the EDC external DAAC Production network address space:

a. Design network and Firewall address changes. Based upon the new external Production network addresses, modify the current network and firewall designs.

b. Coordinate changed addresses with external data providers. Coordinate with ASTER, LPS, and MODAPS so that they are aware that the external Production network addresses are changing, what they are changing too, and when they are changing.

c. Coordinate changed addresses with other DAACs. Coordinate with the other DAACs so that they are aware that the external Production network addresses are changing, what they are changing too, and when they are changing.

d. Modify and verify DNS changes. Edit the DNS tables on the SMC firewall to reflect the new external EDC Production network DNS servers addresses. Verify the changes by performing an nslookup for the domain edcb.ecs.nasa.gov DNS server.

e. Modify and verify external DAAC DNS changes. Edit the forward and reverse DNS tables on the EDC firewall to reflect the new external Production network addresses. Verify changes by performing forward and reverse lookups on the DNS server. Do this lookup for every host on the external Production network.

f. Modify and verify external DAAC sendmail changes. Update the sendmail configuration in the EDC firewall with the new external IP address. Modify the MX records at the SMC. Verify by sending and receiving mail with another user outside of the EDC DAAC.

g. Modify firewall security rules (including all other DAACs). Update the firewall rule set to match the new external Production network addresses. Update the alias addresses on the external firewall interface. Update the firewall rules at the other DAACs so that the currently trusted relationships which are based upon host addresses continues to function. Verify by performing DAAC-to-DAAC ftp data transfers.

h. Modify Firewall external interface configuration. Update the external firewall interface with the new IP address.

i. Modify and verify ECS router configuration changes. Modify the Network Address Translation table in the router. Modify the router interface IP address. Add route advertisements for the new external Production network address. Verify proper network peering with external networks.

j. Verify communication with external interfaces. Perform testing with ASTER, LPS, and MODAPS.

k. Verify communication with other DAACs. Transfer data from the EDC DAAC to each of the other DAACs.

l. Update SMC documentation. The SMC DNS documentation will be updated, processed by the Configuration Control Board and entered into the Configuration Management system.

m. Update EDC documentation. The following EDC documentation will be updated, processed by the Configuration Control Board and entered into the Configuration Management system:

   1. Firewall
   2. DNS
   3. Network

3.2 Readdress Internal DAAC Network Tasks

The following tasks will be performed to readdress the EDC internal DAAC Production network address space:

a. Modify and verify host IP address and default route. On each host change its IP address and default route. Reboot the host and verify that the addresses are correct.

b. Modify and verify Firewall security rules, and modify internal interface. Update the firewall rule set to match the new internal Production network addresses. Update the internal firewall interface with the new IP address. Verify by performing DAAC-to-DAAC ftp data transfers.

c. Modify and verify internal DNS. Edit the forward and reverse DNS tables to reflect the new internal Production network addresses. Verify changes by performing forward and reverse lookups on both the primary (e0css02) and secondary (e0ins02) DNS servers. Do this lookup for every host on the internal Production network.

d. Modify and verify internal sendmail. Edit the internal sendmail parameters on e0ins01 and the firewall. Verify by sending and receiving mail with another user on the internal Production network and outside the DAAC.

e. Modify TCP/Wrappers. Change the /etc/hosts.allow file on all hosts to accept connections from the new internal IP network address.

f. Verify internal interfaces. Test data transfers between hosts within the internal DAAC Production network.

g. Update EDC documentation. The following EDC documentation will be updated, processed by the Configuration Control Board and entered into the Configuration Management system:

   1. Firewall
   2. DNS
   3. Network

This page intentionally left blank.

4. NSIDC DAAC

4.1 Readdress External DAAC Network Tasks

The tasks defined in this section assume that the firewall has already been implemented. The knowledge gained about all external interfaces discovered during the firewall design and implementation are used for this task. See Figure 4-1, NSIDC DAAC Network with Firewall diagram, for details.

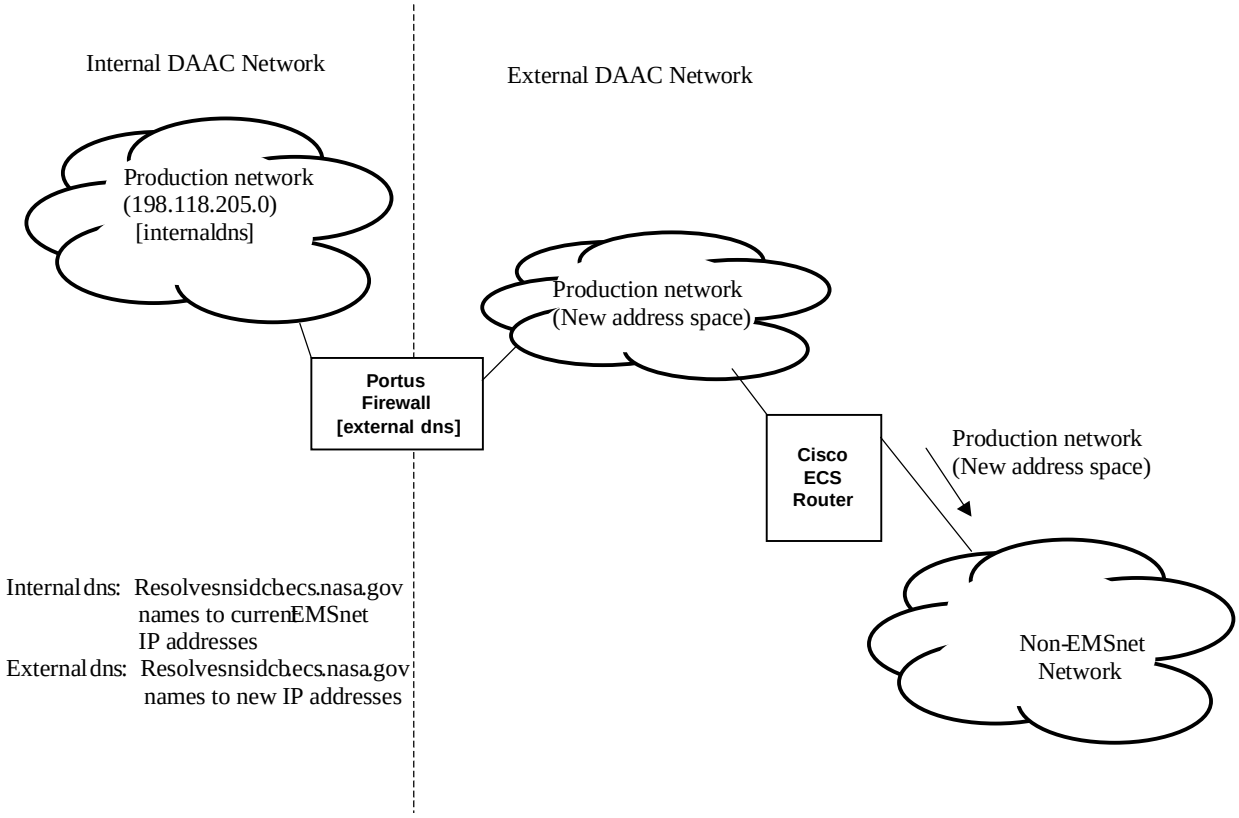

Figure 4-1. NSIDC Network with Firewall

The following tasks will be performed to readdress the NSIDC external DAAC Production network address space:

a. Design network and Firewall address changes. Based upon the new external Production network address, modify the current network and firewall designs.

b. Coordinate changed addresses with external data providers. Coordinate with EDOS, GHRC, I-SIPS, and MODAPS so that they are aware that the external Production network addresses are changing, what they are changing too, and when they are changing.

c. Coordinate changed addresses with other DAACs. Coordinate with the other DAACs so that they are aware that the external Production network addresses are changing, what they are changing too, and when they are changing.

d. Modify and verify DNS changes. Edit the DNS tables on the SMC firewall to reflect the new external NSIDC Production network DNS servers addresses. Verify the changes by performing an nslookup for the domain edcb.ecs.nasa.gov DNS server.

e. Modify and verify external DAAC DNS changes. Edit the forward and reverse DNS tables on the NSIDC firewall to reflect the new external Production network addresses. Verify changes by performing forward and reverse lookups on the DNS server. Do this lookup for every host on the external Production network

f. Modify and verify external DAAC sendmail changes. Update the sendmail configuration in the NSIDC firewall with the new external IP address. Modify the MX records at the SMC. Verify by sending and receiving mail with another user outside of the NSIDC DAAC.

g. Modify firewall security rules (including all other DAACs). Update the firewall rule set to match the new external Production network addresses. Update the alias addresses on the external firewall interface. Update the firewall rules at the other DAACs so that the currently trusted relationships which are based upon host addresses continues to function. Verify by performing DAAC-to-DAAC ftp data transfers.

h. Modify Firewall external interface configuration. Update the external firewall interface with the new IP address.

i. Modify and verify ECS router configuration changes. Modify the Network Address Translation table in the router. Modify the router interface IP address. Add route advertisements for the new external Production network address. Verify proper network peering with external networks.

j. Verify communication with external interfaces. Perform testing with EDOS, GHRC, I-SIPS, and MODAPS.

k. Verify communication with other DAACs. Transfer data from the NSIDC DAAC to each of the other DAACs.

l. Update SMC documentation. The SMC DNS documentation will be updated, processed by the Configuration Control Board and entered into the Configuration Management system.

m. Update NSIDC documentation. The following NSIDC documentation will be updated, processed by the Configuration Control Board and entered into the Configuration Management system:

   1. Firewall
   2. DNS
   3. Network

4.2 Readdress Internal DAAC Network Tasks

The following tasks will be performed to readdress the NSIDC internal DAAC Production network address space:

a. Modify and verify host IP address and default route. On each host change its IP address and default route. Reboot the host and verify that the addresses are correct.

b. Modify and verify Firewall security rules, and modify internal interface. Update the firewall rule set to match the new internal Production network addresses. Update the internal firewall interface with the new IP address. Verify by performing DAAC-to-DAAC ftp data transfers.

c. Modify and verify internal DNS. Edit the forward and reverse DNS tables to reflect the new internal Production network addresses. Verify changes by performing forward and reverse lookups on both the primary (n0css02) and secondary (n0ins02) DNS servers. Do this lookup for every host on the internal Production network.

d. Modify and verify internal sendmail. Edit the internal sendmail parameters on e0ins01 and the firewall. Verify by sending and receiving mail with another user on the internal Production network and outside the DAAC.

e. Modify TCP/Wrappers. Change the /etc/hosts.allow file on all hosts to accept connections from the new internal IP network address.

f. Verify internal interfaces. Test data transfers between hosts within the internal DAAC Production network.

g. Update NSIDC documentation. The following EDC documentation will be updated, processed by the Configuration Control Board and entered into the Configuration Management system:

   1. Firewall
   2. DNS
   3. Network

This page intentionally left blank.

Abbreviations and Acronyms

EBnet	ESDIS Backbone Network
ECS	EOSDIS Core System
EMSnet	ESDIS Mission Support Network

This page intentionally left blank.